IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Godwin et al.
Serial No.	: 09/764,252
Filed	: January 17, 2001
Title	: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR PROVIDING DATA FROM NETWORK SECURE COMMUNICATIONS IN A CLUSTER COMPUTING ENVIRONMENT
Attorney Docket	: 5577-220 (IBM018PA)
Examiner	: A. Patel
Art Unit	: 2154
Confirmation	: 8043

Mail Stop Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S AMENDED BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

Sir:

This Amended Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences", filed January 29, 2007, the Notice of Panel Decision from Pre-Appeal Brief Review, mailed March 29, 2007 and the Notification of Non-Compliant Appeal Brief mailed June 05, 2007. This Amended Appeal Brief provides a clean copy of claim 8 in Appendix A pursuant to the request in the Notification of Non-Compliant Appeal Brief. No other changes have been made relative to the originally filed appeal brief.

Real Party In Interest

The Real Party in Interest in the present Appeal is International Business Machines Corporation Armonk, New York, the assignee, as evidenced by the assignment set forth at Reel/Frame 011496/0142.

Related Appeals and Interferences

The appellant is aware of no appeals or interferences that would be affected by the present appeal.

Status of the Claims

Claims 1-72 are pending in the present application. Claims 2, 10-19, 21, 29-38, 40 and 48-57 have been withdrawn. Claims 1, 3-9, 20, 22-28, 39, 41-47 and 58-72 stand finally rejected by the Examiner as noted in the Final Office Action mailed October 27, 2006 and corresponding Advisory Action mailed January 30, 2007. The rejection of claims 1, 3-9, 20, 22-28, 39, 41-47 and 58-72 is appealed. The claims at issue are attached hereto as Appendix A.

Status of Amendments

Appellant filed a Reply on January 02, 2007 in response to an Office action made Final, which was mailed on October 27, 2006. The Examiner did not enter the Reply as evidenced by the Advisory Action, which was mailed on January 30, 2007.

Summary of Claimed Subject Matter

The claimed invention is directed to providing secure communications over a network in a distributed workload environment having target hosts that are accessed through a distribution processor by a common network address. The distribution processor distributes the workload associated with the client requests among the target hosts, e.g., servers, which are each capable of servicing client requests.

Under certain circumstances, it may be desirable to provide secure communications. For example, Virtual Private Networks (VPN) are becoming increasingly used across the Internet to provide "end-to-end" secure communications, which are secure across the entire communications path between two IP address endpoints. However, Internet security protocols that provide "end-to-end" secure communication present difficulties for load balancing, failure recovery, etc., in a distributed workload environment.

According to aspects of the present invention, secure network communications are handled by processing both inbound and outbound secure network communications at the distribution processor so as to provide network security processing of communications from the target host and network security processing of communications to the target host[1]. For example, the distribution processor may itself, function as the endpoint server for purposes of completing a

[1] See for example, Page 4, para. 35 of appellant's U.S. Pat. Pub. No. 2002/0095603.

secure network communication with a client and may thus perform security processing of information exchanged with a corresponding client[2].

Communications are distributed by the distribution processor for processing by a selected target host (even if the communication is a network secure communication). In this regard, a selected target host may physically reside on the distribution processor itself, or on a separately connected device, e.g., a server computer, etc. As such, communications between the distribution processor and the selected target host which are associated with end-to-end secure network communications are encapsulated. This allows, for example, the distribution processor to distinguish network secure communications from non-secure communications, and may also allow consistent policies to be provided within the environment, which bypass IP filtering for such encapsulated communications.

Independent claim 1 is directed to a method for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 33), the method comprising the steps of:

routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 72; Figs. 4, 5A, 5B);

processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 72, 81, 85, 96; Figs. 4, 5A, 5B);

receiving at the distribution processor, network communications directed to the common network address (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 34, 71; Fig. 4);

encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network

2 See for example, Page 6, para. 71 of appellant's U.S. Pat. Pub. No. 2002/0095603.

communications (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 35, 36, 42, 76, 83, 87, 134, 146); and

distributing the received network communications that are directed to the common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 34, 71; Fig. 4).

Independent claim 20 is directed to a system for providing secure communications over a network in a distributed workload environment having target hosts associated with a common IP address and which are accessed through a distribution processor by a common network address (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 33), comprising:

means for routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 72; Figs. 4, 5A, 5B);

means for processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 72, 81, 85, 96; Figs. 4, 5A, 5B);

means for receiving at the distribution processor, network communications directed to the common network address (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 34, 71; Fig. 4);

means for encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 35, 36, 42, 76, 83, 87, 134, 146); and

means for distributing the received network communications that are directed common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications

among the target hosts (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 34, 71; Fig. 4).

Independent claim 39 is directed to a computer program product for providing secure communications over a network in a distributed workload environment having target hosts associated with a common IF address and which are accessed through a distribution processor by a common network address (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 66), comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 66) comprising:

computer readable program code which routes both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 72; Figs. 4, 5A, 5B);

computer readable program code which processes both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and network security processing of communications to the target host (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 33, 72, 81, 85, 96; Figs. 4, 5A, 5B);

computer readable program code which receives at the distribution processor, network communications directed to the common network address (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 34, 71; Fig. 4);

computer readable program code which encapsulates communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraphs 35, 36, 42, 76, 83, 87, 134, 146); and

computer readable program code which distributes the received network communications that are directed to the common network address among to selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated

with the network communications among the target hosts (See for example, U.S. Pat. Pub. No. 2002/0095603, paragraph 34, 71; Fig. 4).

<u>Grounds of Rejection To Be Reviewed On Appeal</u>

1. Whether Claims 1, 3-9, 20, 22-28, 39, 41-47, 58-72 are unpatentable under 35 U.S.C. § 112, second paragraph.

2. Whether Claims 1, 7, 20, 26, 39, 45 and 58-72 are unpatentable under 35 U.S.C. §102(e) over U.S. Pat. No. 6,266,335 to *Bhaskaran*.

3. Whether Claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and 47 are unpatentable under 35 U.S.C. §103(a) over *Bhaskaran* in view of U.S. Pat. No. 6,826,559 to *Shaffer et al.*

<u>Arguments</u>

1. Grounds of rejection under 35 U.S.C. § 112, second paragraph

1. A. Introduction to 35 U.S.C. §112, second paragraph Analysis

According to the M.P.E.P. §2173.02, a claim element is definite within the meaning of 35 U.S.C. §112, second paragraph, if the claim language provides at least a *reasonable degree* of particularity and distinctness. Some latitude in the manner of expression and the aptness of terms should be permitted even though the claim language is not as precise as the examiner might desire. Moreover, in reviewing a claim for compliance with 35 U.S.C. §112, second paragraph, the Examiner must consider the claim *as a whole* to determine whether the claim apprises one of ordinary skill in the art of its scope[3].

1. B. Claims 1, 3-9, 20, 22-28, 39, 41-47, 58-72 are Definite in view of 35 U.S.C. § 112, second paragraph

The Examiner rejected each of the independent claims, 1, 20 and 39 under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. The remainder of the claims, 3-9, 22-28, 41-47, 58-72

---

[3] See for example, *<u>Orthokinetics, Inc. v. Safety Travel Chairs, Inc.</u>*, 806 F.2d 1565, 1576, 1 USPQ2d 1081, 1088 (Fed. Cir. 1986).

were rejected under §112, second paragraph by virtue of being dependent upon a base claim that was also rejected.

Claim 1 is a method claim, claim 20 is a system claim and claim 39 is a computer program product claim that each currently include the same recitations that the Examiner cited as the basis of the rejections under 35 U.S.C. § 112, second paragraph. As such, these claims shall be discussed together.

Analysis of Claims 1, 20 and 39 under 35 U.S.C. § 112, second paragraph

The Examiner argues that there is insufficient antecedent basis for the recitations: "to distribute workload associated with <u>the network communications</u> among the target hosts", which appears in each of claims 1, 20 and 39. In support of the rejection, the Examiner argues that it is unclear how other "types" of communications recited in the claims are associated with or represented by network communications[4].

The Examiner further argues that there is insufficient antecedent basis for the recitation of "<u>the selection</u> among <u>the target hosts</u>", which appears in each of claims 1, 20 and 39. In support of the rejection, the Examiner argues that it is unclear what the distinction is between the selected hosts and "selected ones of the plurality of target hosts which are associated with end-to-end secure network communications as claimed[5].

The appellant respectfully traverses these rejections. As noted above in the summary, various aspects of the present invention address distributed workload environments in which a given communication may be a non-secure communication, or the communication may be a secure communication.

For example, representative Claim 1 recites a method for providing secure communications over a network in a distributed workload environment having target hosts which

[4] See Office action mailed 10-27-2006, Page 2.
[5] See Office action mailed 10-27-2006, Pages 2-3.

are accessed through a distribution processor by a common network address. The method comprises:

> routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;
>
> processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host;
>
> receiving at the distribution processor, network communications directed to the common network address;
>
> encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications; and
>
> distributing the received network communications that are directed to the common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts.

Initially, with reference to the third and fifth recitations (receiving and distributing), <u>network communications</u> that are directed to the common network address are *received* at the distribution processor, and the distribution processor distributes the received (inbound) network communications that are directed to the common network address among *selected ones of the target hosts* so as to distribute the workload associated with the network communications among the target hosts.

There are numerous ways that a load balancer may chose to distribute the workload across target hosts. As just a few illustrative examples, the load balancer may decide to assign all tasks to a single host device until that host device is at a certain capacity. The workload may be distributed evenly across one or more target hosts, the workload distribution may be weighted, etc. Moreover, certain of the target hosts may be reserved, off-line, or otherwise not participating in load balancing at a given time. Thus, the received network communications directed to the common network address are distributed among "selected ones of the target hosts", e.g., as determined by the particular load balancing techniques that are being implemented.

It is possible that a given network communication may be a non-secure network communication. However, it is also possible that a given network communication is an end-to-end secure network communication[6]. With reference to the first and second recitations (routing and processing), if a network communication is also an end-to-end secure network communication, both inbound and outbound communications with the associated target host are routed through the distribution processor[7]. Further, both inbound and outbound end-to-end secure network communications are processed at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host[8].

As noted in the appellant's specification, certain workload distribution methods experience compatibility problems with end-to-end security, such as the Internet Protocol Security Architecture (IPSec) technology[9]. Compatibility issues with end-to-end security, such as IPSec, in certain workload distribution methods are also recognized in *Bhaskaran*[10], which was cited by the Examiner in rejecting the claims as described in greater detail herein.

However, compatibility issues with end-to-end secure network communications are addressed, as claimed, by processesing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host.

With reference to the fourth recitation (encapsulating), if a network communication is also a secure network communication, the client request must still be satisfied by the distributed workload environment. As such, communications between the distribution processor and

---

See the applicant's published patent application U.S. Pat. Pub. No. US2002/0095603, paragraph 0022-32. See also, U.S. Pat. No. 6,266,335 to *Bhaskaran,* Col. 2, lines 43-58

[7] As noted in the appellant's specification, for non-secure network communications, return communications from a selected target host to the associated client need not pass through the distribution processor – see for example, appellant's U.S. Pat. Pub. No. US2002/0095603, paragraph 72.

[8] See for example, the appellant's U.S. Pat. Pub. No. US2002/0095603, paragraphs 22-32.

[9] See for example, the appellant's U.S. Pat. Pub. No. US2002/0095603, paragraph 32.

[10] See U.S. Pat. No. 6,266,335 to *Bhaskaran,* Col. 2, lines 43-58.

selected ones of the plurality of target hosts which are associated with end-to-end secure network communications are encapsulated.

As an example, encapsulation, such as prior to distribution within the target hosts may provide for simplified filter policies on the data processing systems as it may allow for the efficient separation of communications associated with secure network communications from other communications[11].

The examiner's focus during examination of claims for compliance with the requirement for definiteness of 35 U.S.C. 112, second paragraph, is whether the claims meet the threshold requirements of clarity and precision, not whether more suitable language or modes of expression are available. The essential inquiry pertaining to this requirement is whether the claims set out and circumscribe a particular subject matter with a reasonable degree of clarity and particularity. Definiteness of claim language must be analyzed in light of the content of the particular application disclosure, the teachings of the prior art and the claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made[12].

The appellant believes that, when reading claims 1, 20 and 39, each as a whole, the terms and recitations therein set out and circumscribe the claimed invention with clarity and particularity. Moreover, the claims are reasonably clear to one of ordinary skill in the art, thus the claims meet the statutory requirements of 35 U.S.C. §112, second paragraph. For the reasons set out above, the appellant respectfully requests that the Board reverse the Examiner's final rejection of claims 1, 3-9, 20, 22-28, 39, 41-47, 58-72 under 35 U.S.C. § 112, second paragraph.

2. Grounds of rejection under 35 U.S.C. §102(e) over U.S. Pat. No. 6,266,335 to *Bhaskaran*.

2. A. Introduction to 35 U.S.C. §102(e) Analysis

[11] See for example, appellant's U.S. Pat. Pub. No. US2002/0095603, paragraph 83.
[12] See the M.P.E.P §2173.02.

Claims 1, 7, 20, 26, 39, 45 and 58-72 were rejected under 35 U.S.C. §102(e) as being unpatentable over U.S. Pat. No. 6,266,335 to *Bhaskaran*. Of the rejected claims, claims 1, 20 and 39 are in independent form. According to the M.P.E.P. §706.02, in order to be anticipating under §102, the reference must teach every aspect of the claimed invention[13].

2. B. *Bhaskaran* Fails to Establish a Prima Facie Case of Anticipation

Of the claims rejected under 35 U.S.C. §102(e), Claims 1, 20 and 39 are in independent form. The appellant respectfully asserts that *Bhaskaran* fails to teach or suggest one or more elements needed to establish a *prima facie* case of anticipation with regard to each of the rejected claims[14]. For example:

***Bhaskaran* Fails to Teach Processing Both Inbound and Outbound End-To-End Secure Network Communications as claimed**

With regard to claim 1, *Bhaskaran* fails to teach or suggest:

> … processing both inbound and outbound end-to-end secure network communications *<u>at</u>* the distribution processor <u>so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host</u>…

Similarly, with regard to claim 20, *Bhaskaran* fails to teach or suggest:

> …means for processing both inbound and outbound end-to-end secure network communications *<u>at</u>* the distribution processor <u>so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host</u>…

Still further, with regard to claim 39, *Bhaskaran* fails to teach or suggest:

> …computer readable program code which processes both inbound and outbound end-to-end secure network communications *<u>at</u>* the distribution processor <u>so as to provide endpoint network security processing of communications from the target host and network security processing of communications to the target host</u>…

---

[13] See also *Carella v. Starlight Archery and Pro Line Co.*, 804 F.2d 135, 138, 231 U.S.P.Q. 644, 646 (Fed. Cir. 1986).
[14] See for Example, the M.P.E.P. §706.02(j).

As each of claims 1, 20 and 39 include similar recitations that the appellant believes to be neither taught nor suggested by *Bhaskaran,* these claims shall be discussed together.

In making the above rejections, the Examiner argues that the claimed distribution processor reads on the flow switch 205 disclosed in *Bhaskaran*, and concludes that *Bhaskaran* teaches processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host, citing col. 5, lines 47-51 of *Bhaskaran*[15]. However, the appellant respectfully traverses the Examiner's interpretation of the flow switch 205 in *Bhaskaran.* As will be described in greater detail below, *Bhaskaran* not only fails to teach the claimed invention, but rather teaches away from the claimed invention.

Bhaskaran teaches a distributed workload environment where a flow switch is utilized, e.g., instead of a router, to perform load balancing. The use of a flow switch further allows the disclosed distributed system to participate in network secure communications such as using IPSec. However, as will be seen, *Bhaskaran* neither teaches nor suggests aspects of the claimed invention.

Bhaskaran describes that in order to perform endpoint network security processing, a flow switch/load balancer/distribution processor must decrypt packets communicated from the client. However, decryption requires a non-public crypto-key[16].

The flow switch in *Bhaskaran* manages to perform load balancing in a way that *avoids* the need to perform endpoint network security processing, e.g., obtaining a nonpublic crypto-key and decrypting the client message. As such, the flow switch 205, *per se*, cannot perform endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host as claimed.

---

[15] See the Office action made final, mailed 10/27/2006, pages 6-7.
[16] See for example, *Bhaskaran*, Col. 5, lines 43-65.

To see how *Bhaskaran* performs load balancing in a way *that intentionally avoids* using the flow switch 205 to perform endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host as claimed, reference is first made to Fig. 2 of *Bhaskaran*, which is reproduced below. As shown in Fig. 2 of *Bhaskaran,* a flow switch 205 allows multiple IP servers 290 in a cluster 200 to share the same IP address (IP 192.31.65.1 in the example of Fig. 2)[17]. Note that while each IP server 290 has the same IP address, each server has a unique Layer 2 MAC address (e.g., 126.1, 126.2, 126.3, 126.4, 126.5 as shown in Fig. 2) [18]. As such, the flow switch can select among the servers 290 based upon a knowledge of their unique MAC address. *Bhaskaran* refers to routing based upon the layer 2 MAC address as *Data Link Layer address* translation of packets flowing from an IP client to a selected one of the IP servers in the cluster[19].

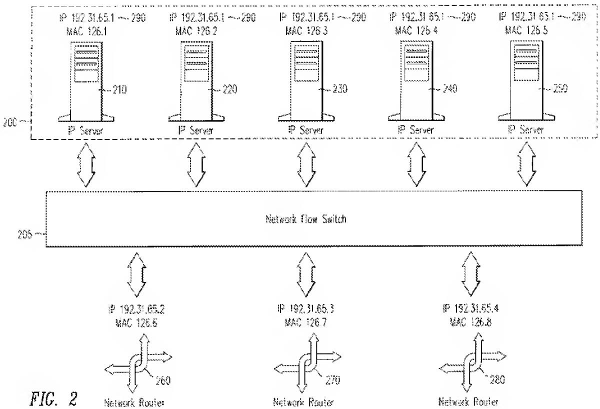

FIG. 2

[17] This is different from the disclosed prior art arrangement where a "load balancer" 100 is coupled to a server cluster where each server has a unique IP (layer 3) address (192.31.65.1 - 192.31.65.5) as seen in Fig. 1 of *Bhaskaran*.

[18] See for example, *Bhaskaran*, Col. 5, lines 47-54.

[19] See for example, *Bhaskaran*, Col. 5, lines 34-37.

The format of a packet transmitted over the external network is illustrated in FIG. 3A, 3B of *Bhaskaran*, which is reproduced below. Fig. 3A has been modified herein to include additional relevant text. Notably, the packet 300 includes a link field 320, an IP header 330, a TCP header 340, a data payload 350, a CRC field 360 and a trailer 370. IP header 330 and TCP header 340 are standard IP and TCP headers. The CRC field 360 contains a checksum correction code used to verify that packet 300 has been transmitted without error[20]. FIG. 3B illustrates the format of link field 320, which includes Layer 2 information, including a Data Link Layer source address field 380 (MAC source address), a Data Link Layer destination address (MAC destination address) field 390 and type field 395[21].

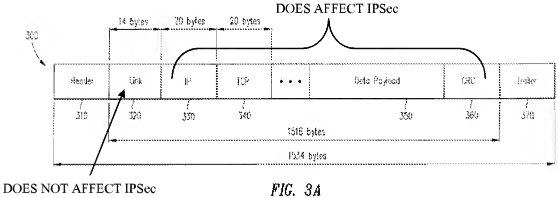

FIG. 3A

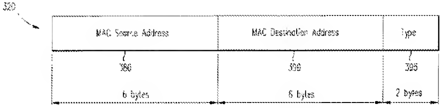

FIG. 3B

An inbound communication received at the flow switch 205 specifies a virtual IP address. To perform load balancing and flow control, the flow switch 205 selects a server 290. This can be accomplished because the flow switch 205 knows the unique MAC address (layer 2) of each

---

[20] See for example, *Bhaskaran*, Col. 6, lines 27-50.
[21] See for example, *Bhaskaran*, Col. 6, lines 27-50.

server in the cluster. The flow switch 205 then routes packets to the selected server by performing data link layer address translation, i.e., writing the MAC address (Layer 2) of the selected server into the Data Link Layer (MAC) destination address[22] (field 390 of each packet 300 as seen in Fig. 3B corresponding to the link field 320 in Fig. 3A)[23], and by forwarding the packet on to the appropriate server.

This ability of the flow switch 205 to perform data link layer address translation allows the flow switch 205 to route packets to a selected server without "disrupting" the flow of an end-to-end secure network communication from the client to a corresponding one of the selected servers 290 because the flow switch 205 can route *and load balance* without acting like an endpoint and without modifying fields of the packet involved in end-to-end network security, thus avoiding violations of end-to-end secure network communications[24].

To understand the significance of this aspect of *Bhaskaran,* only a very basic understanding of end-to-end network secure communications is necessary. An end-to-end network secure communication, such as using IPSec technology, operates on the network layer (layer 3) in conjunction with an Internet Key Exchange (IKE) protocol component[25]. The operation of IPSec on layer 3 of a network communication is further described explicitly in *Bhaskaran,* which discloses that the transport layer (layer 4) is provided as part of the network layer (layer 3) payload which is completely encrypted in an IPSec implementation[26]. Also, in IPSec, encryption is performed at the client and decryption is performed at the server using secret crypto-keys that are unique to each client-server link[27] and vise versa (end-to-end security).

---

[22] See for example, *Bhaskaran*, Col. 5, lines 34-37.
[23] See for example, *Bhaskaran*, Col. 5, lines 56-63.
[24] *Bhaskaran* discloses a conventional approach in Fig. 1, where each server has its own unique IP address. However, network secure communications such as IPSec fail in this conventional approach because the router/load balancer must replace the virtual IP address in the packet received from the client with the IP address of the selected server. This requires the load balancer to open the packet and recompute the checksum, which cannot be performed because the payload of the packet is encrypted as part of the IPSec security. As such, load balancing fails for IPSec and other communications that encrypt the payload.
[25] See for example, the applicant's U.S. Pat. Pub. No. US2002/0095603, paragraph 0022.
[26] See for example, *Bhaskaran*, Col. 2, lines 43-65.
[27] See for example, *Bhaskaran*, Col. 2, lines 52-55.

<u>*Bhaskaran Expressly Teaches Away From the Flow Switch Performing Endpoint Processing*</u>

There is no teaching or suggestion anywhere in *Bhaskaran* that describes the flow switch 205 processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host. In fact, *Bhaskaran* expressly teaches that the flow switch 205 avoids acting as an endpoint.

As noted in *Bhaskaran*:

> … If IP header 330 were modified… the checksum for CRC field 360 would have to be recalculated, an operation requiring processor intervention. In addition, if encrypted information is transmitted according to the IPSEC security framework, decryption of the IP payload is required. <u>*Thus, by eliminating the need to recompute the checksum for each packet*</u>, the network flow switch of the present invention achieves better throughput than prior art devices. Network owners can further deploy IPSEC security mechanisms transparently and without fear of communications being broken[28]. (emphasis added)

The "better throughput" noted by *Bhaskaran* is derived from the observation that the flow switch 205 can simply <u>*pass*</u> packets with encrypted payloads to the assigned IP server <u>*without providing*</u> endpoint network security processing as claimed[29]. Since all servers 290 share the same IP address, there is no need to modify any layer 3 information, e.g., the IP address, payload or checksum that participate in IPSec. Instead, the job of endpoint secure communication processing must be left to the selected server 290. Thus, end-to-end secure network communications such as IPSec are unaffected by the decisions of the flow switch 205.

The Examiner further concludes that the flow switch 205 must serve as an endpoint as claimed and cites several passages in *Bhaskaran* that disclose IPSec[30]. However, as clarified above, the fact that IPSec can be performed in the invention in *Bhaskaran* neither teaches nor suggests the claimed invention. Indeed, the "fear of communications being broken" disclosed in

---

[28] See *Bhaskaran*, Col. 6, lines 38-50.

[29] Since link field 320 is not part of the IP protocol, there is no need to recalculate the checksum for CRC field 360 when link field 320 is modified.

[30] See for example, Office action mailed 10-27-2006, Pages 5-7; Advisory Action mailed 1/30/2007, pages 3-5.

Bhaskaran is avoided because the selected IP server 290 (*and not the flow switch 205*) is the endpoint for both inbound and outbound packets.

Because the flow switch 205 does not have to peek into the packet payload or otherwise have to modify the IP address to perform load balancing, broken communications and other interoperability issues with network secure communications are transparent because the flow switch merely passes packets to the endpoint server in the cluster so that the *server 290 is* the endpoint for secure communication. Since the link field 320 containing the (layer 2) MAC address *does not participate in IPSec*, there is no "fear of communications being broken" when link field 320 is modified[31].

Accordingly, *Bhaskaran* does not teach or suggest processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications as claimed.

***Bhaskaran* Fails to Teach Encapsulating Communications as claimed**

With regard to claim 1, *Bhaskaran* fails to teach or suggest:

... encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications...

With regard to claim 20, *Bhaskaran* fails to teach or suggest:

...means for encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications...

With regard to claim 39, *Bhaskaran* fails to teach or suggest:

...computer readable program code which encapsulates communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications...

---

[31] See also, *Bhaskaran*, Col. 2, lines 43-65.

In support of the rejection, the Examiner cites *Bhaskaran, Col. 4, lines 19-28*[32]. This passage has absolutely nothing to do with encapsulating packets at all, but rather recites that the flow switch 205 can perform load balancing, fault tolerance, etc.

Encapsulation is not taught or suggested. Moreover, *Bhaskaran* explicitly teaches that even if the flow switch 205 is used in a duplex operation, there is no need to manipulate outbound packets at all. Rather, the flow switch may be used for duplex for example, to address outbound load balancing to the routers, to address issues flow when a router becomes unavailable, etc[33].

Accordingly, *Bhaskaran* does not teach or suggest encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications as claimed.

The appellant believes that claims 1, 20 and 39 are patentable over *Bhaskaran* at least for the reasons set out above. The appellant further believes that the remainder of the rejected claims are also patentable over *Bhaskaran,* at least by virtue of being dependent upon one of the base claims discussed above. For the reasons set out above, the appellant respectfully requests that the Board reverse the Examiner's final rejection of claims 1, 7, 20, 26, 39, 45 and 58-72 under 35 U.S.C. §102(e).

3. Grounds of rejection under 35 U.S.C. §103(a) over B*haskaran in view of U.S. Pat. No. 6,826,559 to Shaffer et al. (hereinafter, Schaffer).*

3. A. Introduction to 35 U.S.C. §103(a) Analysis

According to the M.P.E.P. §706.02(j), to establish a *prima facie* case of obviousness, the prior art reference must teach or suggest all the claim limitations[34]. It is the appellant's position

[32] See the Office action made final, mailed 10/27/2006, page 7.
[33] See Bhaskaran, Col. 8, lines 8-65.
[34] See also, *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143 - § 2143.03

that a *prima facie* case of obviousness has not been established for the claims set out herein as these claims depend from one of claims 1, 20 or 39, which appellant now believes are patentable over the art of record.

Claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over *Bhaskaran* in view of U.S. Pat. No. 6,826,599 to Shaffer et al. (hereinafter, *Schaffer*).

The appellant believes that the cited references, even when combined, fail to teach or suggest all of the limitations of the above claims. For example, each rejected claim depends from a base claim (1, 20 or 39), which the appellant has already discussed above. Moreover, With regard to claim 1, *Bhaskaran* combined with *Schaffer* fails to teach or suggest:

> … processing both inbound and outbound end-to-end secure network communications *at* the distribution processor <u>so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host</u>…

Similarly, with regard to claim 20, *Bhaskaran* combined with *Schaffer* fails to teach or suggest:

> …means for processing both inbound and outbound end-to-end secure network communications *at* the distribution processor <u>so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host</u>…

Still further, with regard to claim 39, *Bhaskaran* combined with *Schaffer* fails to teach or suggest:

> …computer readable program code which processes both inbound and outbound end-to-end secure network communications *at* the distribution processor <u>so as to provide endpoint network security processing of communications from the target host and network security processing of communications to the target host</u>…

Shaffer is completely silent with regard to, and does not teach or suggest a distribution processor or processing inbout and outbound end-to-end secure network communications.

Still further, with regard to claim 1, *Bhaskaran* combined with *Schaffer* fails to teach or suggest:

… encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications…

With regard to claim 20, *Bhaskaran* combined with *Schaffer* fails to teach or suggest:

…means for encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications…

With regard to claim 39, *Bhaskaran* combined with *Schaffer* fails to teach or suggest:

…computer readable program code which encapsulates communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications…

For example, *Schaffer* teaches techniques for handling objects in a network cache using a cost function. A cache enabled router reads a packet header and decides whether the packet is a TCP packet. If the packet is a TCP packet and the packet is destined for port 80, the router encapsulates the packet and sends it to a selected cache by adding another TCP header that specifies the selected cache as the destination address[35]. As such, even though a packet is "encapsulated", this is only to direct the packet to a network cache and is not between a distribution processor and a target host.

For the reasons set out above, the appellant respectfully requests that the Board reverse the Examiner's final rejection of claims 3-6, 8, 9, 22-25, 27, 28, 41-44, 46 and under 35 U.S.C. §103(a).

[35] See for example, *Shaffer*, Col. 5, line 45 through Col. 6, line 10 and Fig. 3.

Conclusion

For all of the above reasons, the appellant respectfully submits that the pending claims claims define patentably over the applied prior art. Accordingly, it is respectfully requested that the Board reverse the Examiner's final rejection of claims 1, 3-9, 20, 22-28, 39, 41-47 and 58-72.

Respectfully submitted,

Stevens & Showalter, L.L.P.

By

/Thomas E. Lees/

Thomas E. Lees Reg. No. 46,867

7019 Corporate Way
Dayton, Ohio 45459-4238
Phone 937-438-6848
Fax 937-438-2124

June 26, 2007

Appendix A – Claims Appendix

1. (previously presented) A method for providing secure communications over a network in a distributed workload environment having target hosts which are accessed through a distribution processor by a common network address, the method comprising the steps of:

routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host;

receiving at the distribution processor, network communications directed to the common network address;

encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications; and

distributing the received network communications that are directed to the common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts.

2. (canceled).

3. (previously presented) A method according to Claim 1, further comprising the steps of:

determining if the received network communications are end-to-end secure network communications which are to be distributed to ones of the target hosts;

wherein encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises processing the received network communications so as to provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are end-to-end secure network communications which are distributed

to ones of the target hosts and to not provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are not end-to-end secure network communications.

4. (previously presented) A method according to Claim 3, wherein processing both inbound and outbound end-to-end secure network communications further comprises the steps of:

receiving at the distribution processor communications from the ones of the target hosts which are associated with end-to-end secure network communications; and

processing the received communications from the ones of the target hosts so as to provide endpoint network security for the communications from the ones of the target hosts.

5. (previously presented) A method according to Claim 1, wherein encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises encapsulating the communications in a generic routing format.

6. (previously presented) A method according to Claim 5, wherein the generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distribution processor and ones of the plurality of target hosts.

7. (previously presented) A method according to Claim 1, wherein the communications received from the target hosts at the distribution processor and the encapsulated communications to ones of the plurality of target hosts from the distribution processor are communicated over trusted communication links.

8. (previously presented) A method according to Claim 5, further comprising establishing common IP filters for communications at the distribution processor and the plurality or target hosts.

9. (original) A method according to Claim 8, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

10-19. (canceled).

20. (previously presented) A system for providing secure communications over a network in a distributed workload environment having target hosts associated with a common IP address and which are accessed through a distribution processor by a common network address, comprising:

means for routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

means for processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and endpoint network security processing of communications to the target host;

means for receiving at the distribution processor, network communications directed to the common network address;

means for encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications; and

means for distributing the received network communications that are directed common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts.

21. (canceled).

22. (previously presented) A system according to Claim 20, further comprising:

means for determining if the received network communications are end-to-end secure network communications which are to be distributed to ones of the target hosts;

wherein the means for encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprise means for processing the received network communications so as to provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are secure network communications which are distributed to ones of the target hosts and means to not provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are not end-to-end secure network communications.

23. (previously presented) A system according to Claim 22, wherein the means for processing both inbound and outbound end-to-end secure network communications further comprises:

means for receiving at the distribution processor communications from the ones of the target hosts which are associated with end-to-end secure network communications; and

means for processing the received communications from the ones of the target hosts so as to provide endpoint network security for the communications from the ones of the target hosts.

24. (previously presented) A system according to Claim 20, wherein the means for encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises means to encapsulate the communications in a generic routing format.

25. (previously presented) A system according to Claim 24, wherein generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distributing processor and ones of the plurality of target hosts.

26. (previously presented) A system according to Claim 20, wherein the communications received from the target hosts and the encapsulated communications to ones of the plurality of target hosts are communicated over trusted communication links.

27. (previously presented) A system according to Claim 24, further comprising means for establishing common IP filters for communications at the distributing processor and the plurality of target hosts.

28. (original) A system according to Claim 27, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

29.-38. (canceled).

39. (previously presented) A computer program product for providing secure communications over a network in a distributed workload environment having target hosts associated with a common IF address and which are accessed through a distribution processor by a common network address, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which routes both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor;

computer readable program code which processes both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications from the target host and network security processing of communications to the target host;

computer readable program code which receives at the distribution processor, network communications directed to the common network address;

computer readable program code which encapsulates communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications; and

computer readable program code which distributes the received network communications that are directed to the common network address among selected ones of the target hosts,

wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts.

40. (canceled).

41. (previously presented) A computer program product according to Claim 39, further comprising:

computer readable program code which determines if the received network communications are end-to-end secure network communications which are to be distributed to ones of the target hosts;

wherein the computer readable program code which encapsulates communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises computer readable program code which processes the received network communications so as to provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are end-to-end secure network communications which are distributed to ones of the target hosts and to not provide encapsulated generic communications to the ones of the plurality of target hosts if the received network communications are not end-to-end secure network communications.

42. (previously presented) A computer program product according to Claim 41, wherein the computer readable program code which processes both inbound and outbound end-to-end secure network communications further comprises:

computer readable program code which receives at the distribution processor communications from the ones of the target hosts which are associated with end-to-end secure network communications; and

computer readable program code which processes the received communications from the ones of the target hosts so as to provide endpoint network security for the communications from the ones of the target hosts.

43. (previously presented) A computer program product according to Claim 39, wherein computer readable program code which encapsulates communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications comprises computer readable program code which encapsulates the communications in a generic routing format.

44. (previously presented) A computer program product according to Claim 43, wherein generic communications are encapsulated in a generic routing format having sufficient information in a header of the generic routing format so as to authenticate the source of the communication between the distributing processor and ones of the plurality of target hosts.

45. (previously presented) A computer program product according to Claim 39, wherein the communications received from the target hosts at the distribution processor and the encapsulated communications to ones of the plurality of target hosts from the distribution processor are communicated over trusted communication links.

46. (previously presented) A computer program product according to Claim 43, further comprising computer readable program code which provides common IP filters for communications encapsulated in the generic routing format at the distributing processor and the plurality of target hosts.

47. (original) A computer program product according to Claim 46, wherein the common IP filters bypass IP filtering for inbound communications encapsulated in the generic routing format.

48.-57. (canceled).

58. (previously presented) The method according to Claim 1, wherein distributing the received network communications that are directed to the common IP address among selected ones of the target hosts comprises:

selecting among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts.

59. (previously presented) The method according to Claim 58, wherein selecting among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts comprises:

selecting among the target hosts associated with the common network address based on a round-robin pattern.

60. (previously presented) The method according to Claim 1, wherein distributing the received network communications that are directed to the common network address among selected ones of the target hosts comprises:

selecting among the target hosts for distribution of the network communications in response to a dynamic criteria that changes over time to distribute workload associated with the network communications among the target hosts.

61. (previously presented) The method according to Claim 39, wherein the computer readable program code which distributes the received network communications that are directed to the common network address among selected ones of the target hosts comprises:

computer readable program code that selects among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts.

62. (previously presented) The method according to Claim 61, wherein the computer readable program code that selects among the target hosts for distribution of the network communications in response to a predefined selection pattern to distribute workload associated with the network communications among the target hosts comprises:

computer readable program code that selects among the target hosts associated with the common network address based on a round-robin pattern.

63. (previously presented) The method according to Claim 39, wherein the computer readable program code which distributes the received network communications that are directed to the common network address among selected ones of the target hosts comprises:

computer readable program code that selects among the target hosts for distribution of the network communications in response to a dynamic criteria that changes over time to distribute workload associated with the network communications among the target hosts.

64. (previously presented) The method according to claim 1, further comprising:

receiving at a target host, an encapsulated communication;

comparing a physical link corresponding to said distributor to a source of encapsulation; and

ignoring the encapsulated communication if said physical link does not match to said source of encapsulation.

65. (previously presented) The method according to claim 1, wherein distributing the received network communications that are directed to the common network address among selected ones of the target hosts distribution processor comprises distributing the received network communications using a sysplex distributor.

66. (previously presented) The method according to claim 1, wherein the end-to-end secure network communication comprises a communication using the IPSEC communication protocol.

67. (previously presented) The system according to claim 20, further comprising:

means for receiving at a target host, an encapsulated communication;

means for comparing a physical link corresponding to said distributor to a source of encapsulation; and

means for ignoring the encapsulated communication if said physical link does not match to said source of encapsulation.

68. (previously presented) The system according to claim 20, wherein the means for distributing the received network communications comprises a sysplex distributor.

69. (previously presented) The system according to claim 20, wherein the end-to-end secure network communication comprises a communication using the IPSEC communication protocol.

70. (previously presented) The computer program product according to claim 39, further comprising:

computer readable program code which receives at a target host, an encapsulated communication;

computer readable program code which compares a physical link corresponding to said distributor to a source of encapsulation; and

computer readable program code which ignores the encapsulated communication if said physical link does not match to said source of encapsulation.

71. (previously presented) The computer program product according to claim 39, wherein the computer readable program code which distributes the received network communications comprises a sysplex distributor.

72. (previously presented) The computer program product according to claim 39, wherein the end-to-end secure network communication comprises a communication using the IPSEC communication protocol.

Appendix B – Evidence Appendix

There is no information for this appendix

Appendix C – Related Proceedings Appendix

There is no information for this appendix